

Figure 2

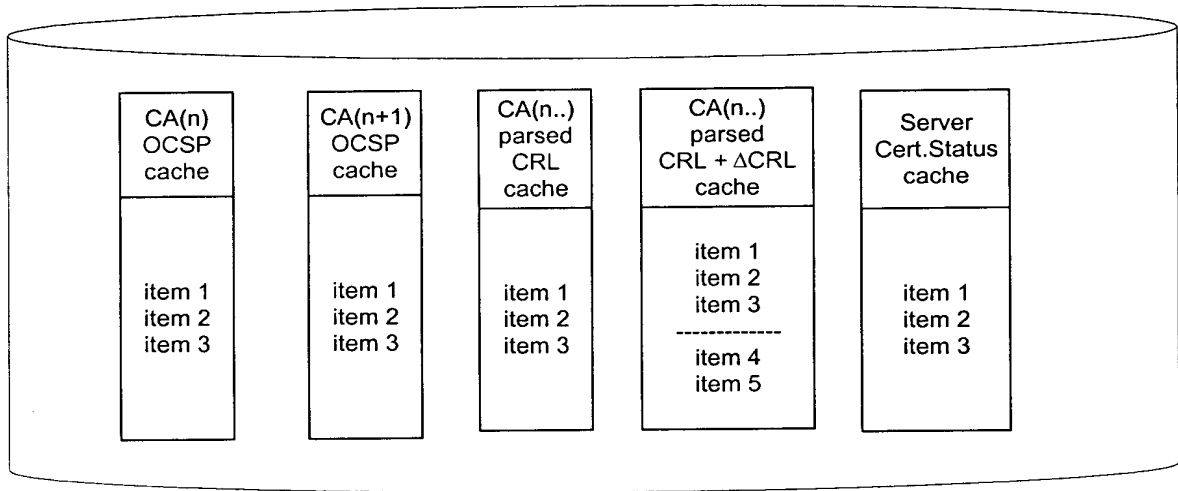


Figure 3

Signature Block Syntax Example

Free form example of data elements making up a digital signature where the signature is applied to multiple message fragments and a date/time stamp. This example is not meant to be taken literally, but is meant to be illustrative of the type of syntax that may be used.

```
<Signature>
  <SignedInfo>
    <Signature Method
      Algorithm = RSA (1024bit)/>
    <ReferenceContent>
      <ReferencetoFragment1>
        <HashAlgorithm = SHA-1>
        <HashValue>A62E...</HashValue>
      </Reference>
      <ReferencetoFragment2>
        <HashAlgorithm = SHA-1>
        <HashValue>F0BC...</HashValue>
      </Reference>
      <Authenticated Data>
        <Date>...</Date>
        <Time>...</Time>
      </Authenticated Data>
      <HashAlgorithm = SHA-1>
      <CumulativeHashValue>6E31...</CumulativeHashValue>
    </ReferenceContent>
  </SignedInfo>
  <SignatureValue>602C...</SignatureValue>
  <Unauthenticated Data>
    <
  </Unauthenticated Data>
  <KeyInfo>
    <X509ParsedData>
      <Sequence of X.509 Data Elements>
        <X509Serial #
        <X509Issuer name
        <..
        <X509Subject name
        <..
      </
    </X509ParsedData>
    <X509Certificate>MIIE...</X509 Certificate>
  </KeyInfo>
</Signature>
```

The <CumulativeHashValue> is the applied to HashValues one or more fragment or the total content and any Authenticated Data.

Figure 4

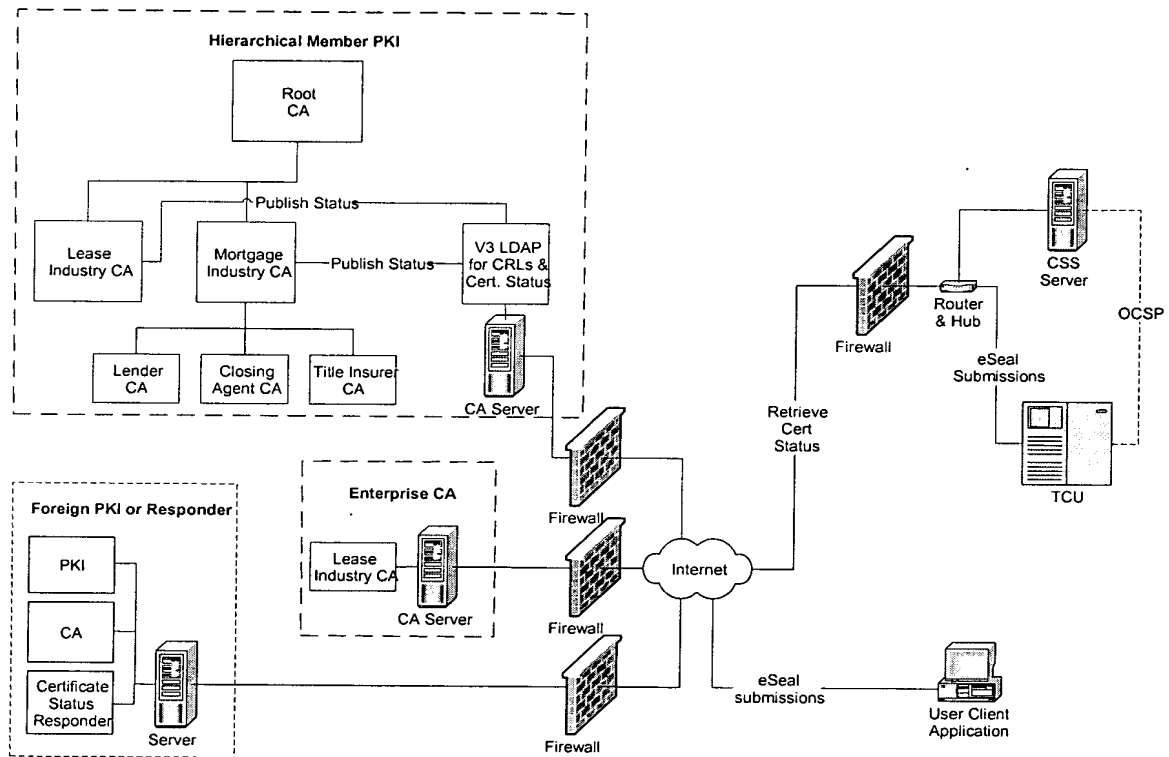


Figure 5

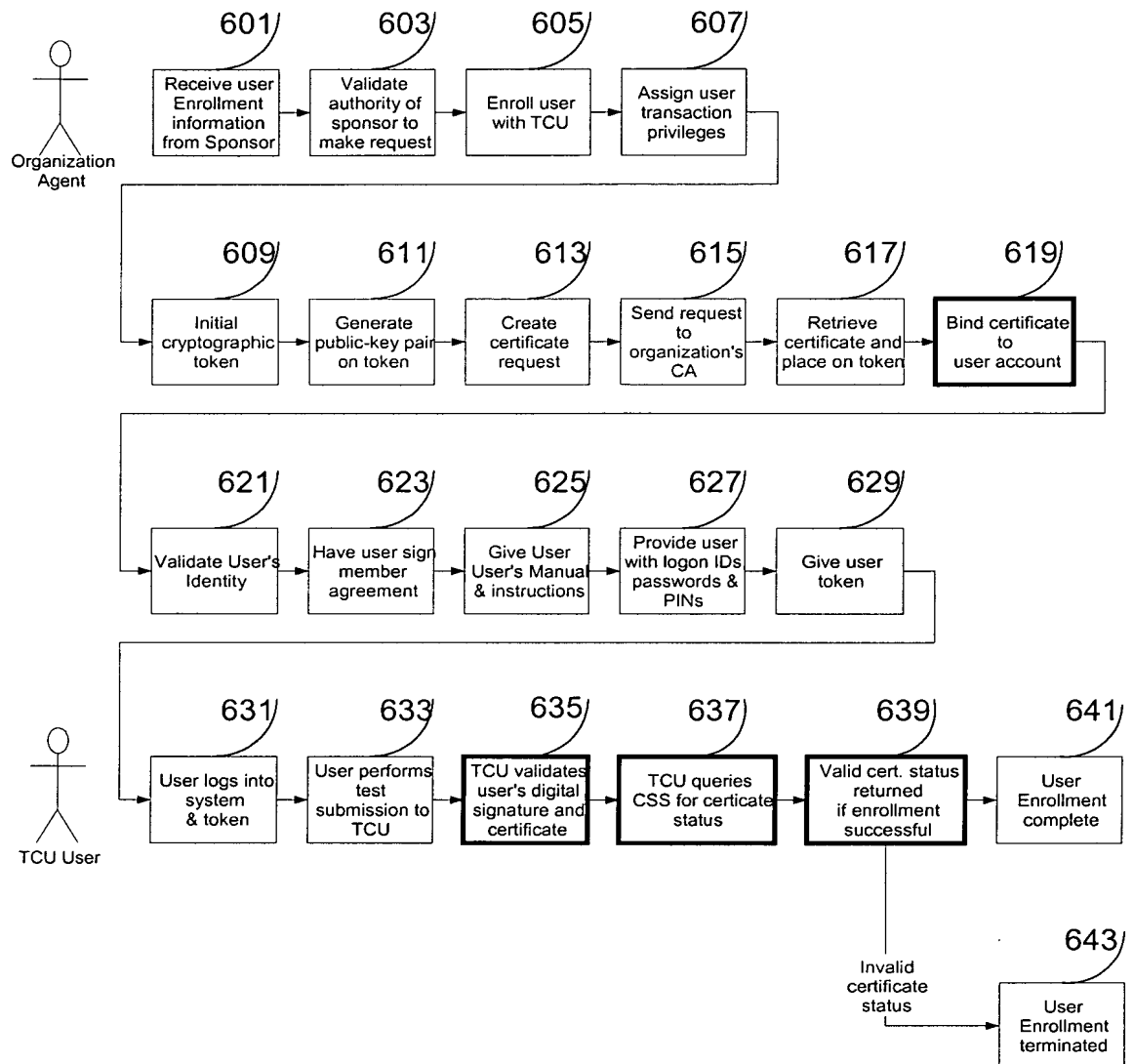


Figure 6

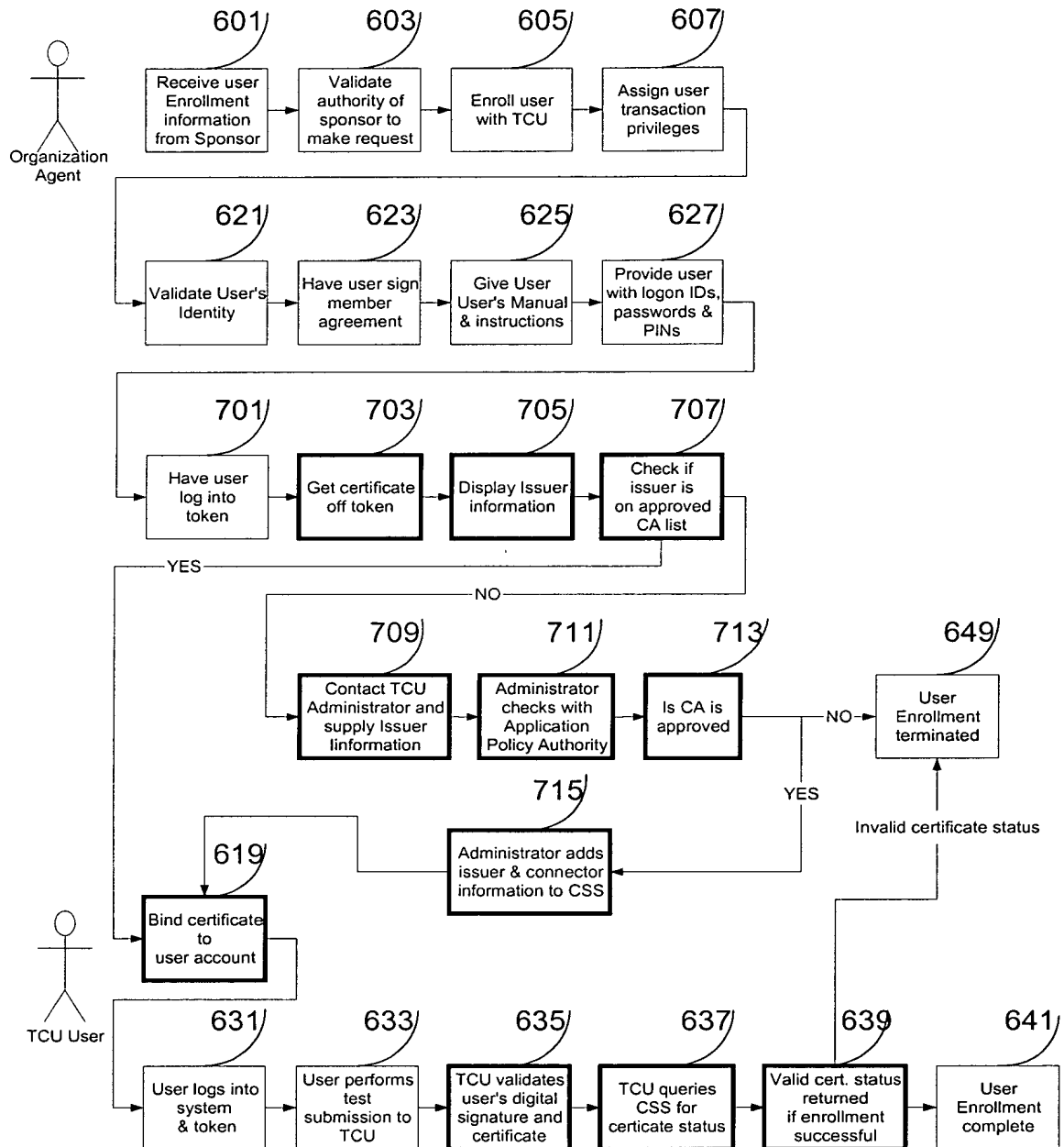


Figure 7

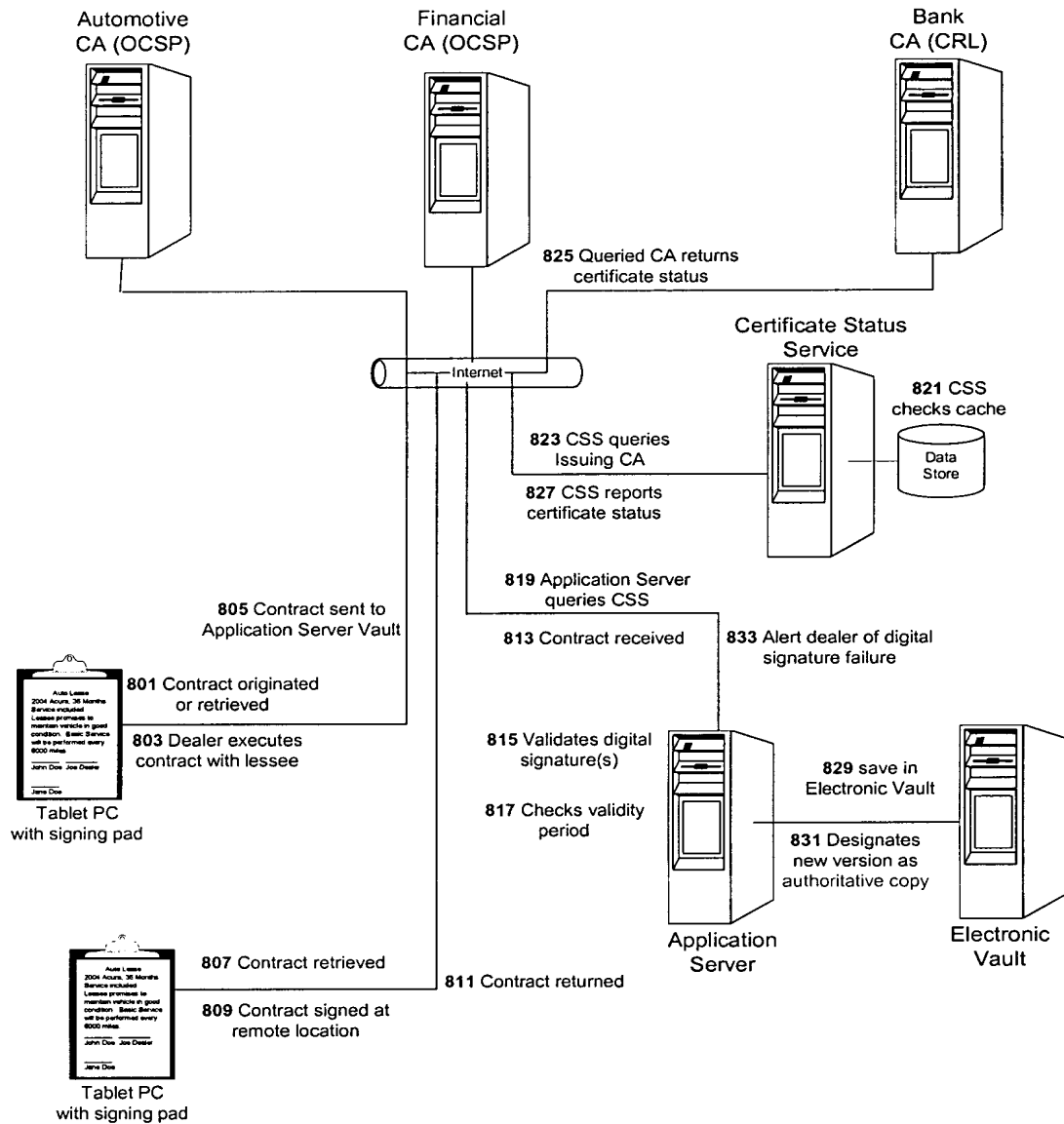


Figure 8